Дополнительные параметры для алгоритмов GSII64

Размер вопроса GrdTransform

Под размером вопроса (поле **Размер вопроса**) в данном случае подразумевается максимальная длина данных на входе операции GrdTransform, которую эта операция может обработать за один прием (ср. с понятием **Размер вопроса алгоритму**).

Для однонаправленных аппаратных алгоритмов длина вопроса GrdTransform – это величина постоянная, в отличие от алгоритмов типа **GSII64,** которые могут принимать от **GrdTransform** блоки данных разной длины:

Режимы работы алгоритма GSII64	Размер вопроса GrdTransform, байтов
ECB и CBC	Число, кратное 8. Максимальное значение – 248
CFB и OFB	Произвольное число, не превышающее 255

Задайте размер вопроса в одноименном поле ввода (значение по умолчанию 8 байтов).

Метод преобразования

Симметричные алгоритмы имеют 4 режима работы, которые отличаются по своим характеристикам и назначению. Подробнее об алгоритмах см. *во 2-й части Руководства пользователя*.

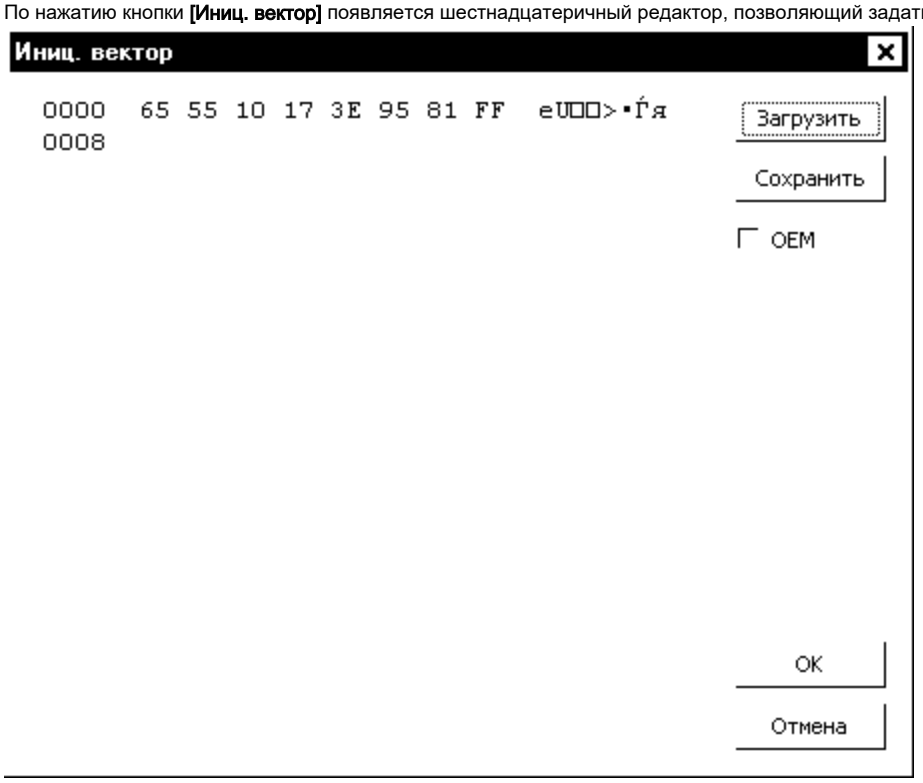
Выберите метод преобразования с помощью одноименного разворачивающегося списка.

Режим преобразования

Выберите направление преобразования (кодирование или декодирование) с помощью одноименного разворачивающегося списка.

Вектор инициализации

По нажатию кнопки **[Иниц. вектор]** появляется шестнадцатеричный редактор, позволяющий задать значение вектора инициализации:



Элементы управления диалога **Вектор инициализации**:

Элемент интерфейса	Назначение

Окно шестнадцатеричного редактора	Ввести значение вектора инициализации
Кнопка **[Загрузить]**	Загрузить дамп из файла с расширением *.dmp
Кнопка **[Сохранить]**	Сохранить дамп в файле с расширением *.dmp
Флаг **OEM**	Выбрать Windows- / DOS-кодировку. По умолчанию используется Windows-кодировка (ANSI) – опция OEM отключена

Зависимость режимов работы симметричного алгоритма от вектора инициализации:

Режимы работы алгоритма AES/GSII64	**Зависимость от вектора инициализации**
ECB	Не зависит
CBC и OFB	Зависят. Для преобразования информации следует использовать один и тот же вектор инициализации. В противном случае данные будут декодированы неверно
CFB	Зависит. Для преобразования информации следует использовать один и тот же вектор инициализации. В противном случае первые 8 байтов данных будут декодированы неверно